FORCEPOINT

产品资料

# Forcepoint NGFW

**FORCEPOINT NGFW 可提供基于情报感知且支持实时更新的高性能安全，能够有效地保护企业网络。这款产品集业内最好的高级规避防范和全面的下一代防火墙保护于一身，无论是对于远程站点、分支机构、数据中心还是网络边缘，都能够提供所需的保护。**

**Forcepoint NGFW** 的最基本功能是提供有效 的保护，它将细粒度的应用控制、入侵防御系统 (IPS)、内置虚拟专用 网 (VPN) 和深度数据包检测整合到一个高效、灵活、高度可扩展的统一设计中。在此基础上增加了强大的防规避技术，能够在检测之前解码并规范化各个协议层的网络流量，从而发现并拦截最先进的攻击方法。

### 拦截复杂的数据泄露攻击

大型数据泄露仍然困扰着各行各业的企业和组织。现在，应用层外泄防护解决方案可以对抗这种情况。借助这个最新的解决方案，下一代防火墙可以根据非常细粒度的端点情景数据有选择性地自动拦截来自 PC、笔记本电脑、服务器、文件共享设备及其他端点设备的网络流量。应用层外泄防护解决方案是目前唯一超越典型的下一代防火墙的解决方案，可防止攻击者试图通过未经授权的程序、Web 应用程序、用户和通信渠道窃取端点设备中的敏感数据。

### 高度的灵活性满足您不断变化的安全需求

下一代防火墙采用统一软核结构，因此能够在瞬息万变的商业环境中轻松变换安全角色（包括防火墙 / VPN、IPS 和第 2 层防火墙）。统一软核结构还优化了数据平面，使得这款产品无论在安全角色还是主动安全功能数量方面，都有很大的性能优势。为了实现更高的灵活性，Stonesoft 下一代防火墙有多种部署方式 —— 可部署为物理设备、软件解决方案、虚拟设备或物理设备上的虚拟情景。

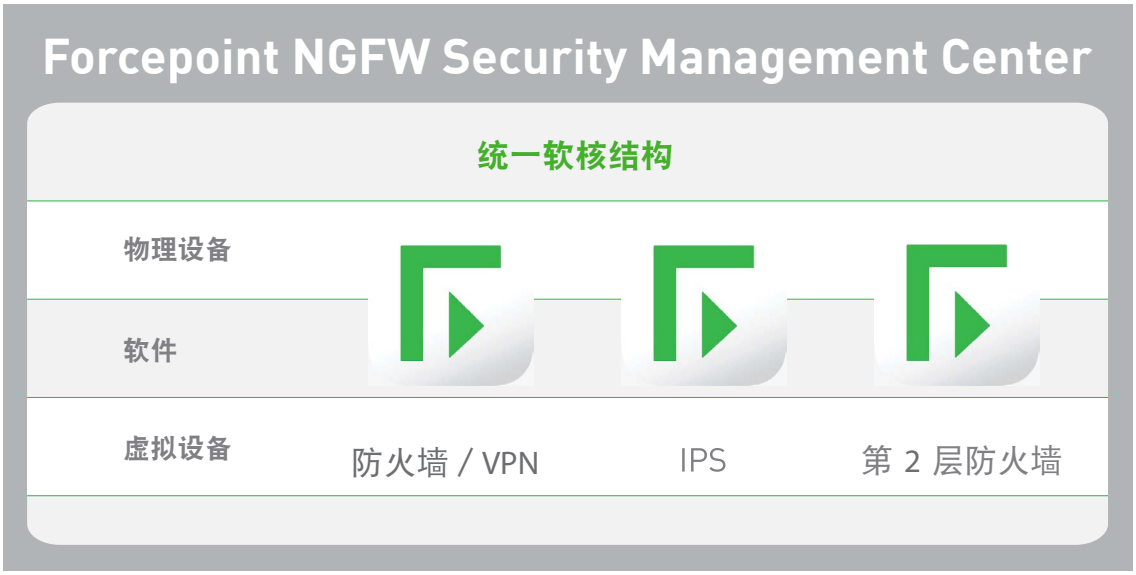
### 高可扩展性和高可用性保护您的关键业务应用

如今，企业需要弹性极高的网络安全解决方案。Forcepoint NGFW 通过以下三种有效方式实现了高可扩展性和高可用性：

- 内置主动 — 主动集群：最多可将 16 个节点集群在一起，在运行要求高的安全应用（例如，深度包检测和 VPN）时，具有出色的性能和弹性。
- 透明会话失效备援：具有行业领先的安全系统可用性和适用性。Stonesoft 下一代防火墙还支持针对同一集群内多个软件和硬件版本的透明失效备援。
- 多链路：使网络连接和 VPN 连接也实现高可用性。每一次部署都可实现高性能，确保全天候的安全防护。

### 为企业提供无以伦比的防护

攻击者用于攻破企业网络、应用程序、数据中心和端点的手段与日俱进。一旦攻破防线，攻击者就可以窃取知识产权、客户信息及其他敏感数据，导致企业的业务和信誉蒙受无法弥补的损失。




有些攻击者会使用高级规避技术来避开如今的大多数网络安全设备。高级规避技术利用掩蔽和混淆等手段，在各个网络层或协议中散播零散的恶意软件。一旦进入到网络，威胁就会重新进行组合，能够持续数日、数月甚至数年地窃取敏感数据而不被发现。

Forcepoint NGFW 将分层威胁发现技术应用于网络流量，能够深入地识别应用程序和用户，因此能够根据业务规则来应用安全策略。然后，它会执行有针对性的深度数据包检测，包括使用全栈规范化等高级技术，以及进行基于水平数据流的检测。这些技术可将流量完全规范化，使得 Forcepoint NGFW 可检测到能够避开其他下一代防火墙的高级规避技术和异常流量。只有在流量完全规范化之后，才能正确地检测各个协议和层中存在的威胁及恶意软件。到目前为止，只有 Forcepoint NGFW 成功地针对 8 亿多种高级规避技术进行了测试。

### 主要优点

- 能够为您的营业资产和数字资产提供最佳保护
- 能够阻止端点数据外泄
- 能够灵活地满足您的安全需求
- 可随着您的业务发展轻松地扩展
- 可提高员工和客户的生产率
- 可降低安全及网络基础设施的总体拥有成本

### 主要特点

- 基于情报感知的安全控制
- 应用层外泄防护
- 高级规避防范
- 统一软核设计
- 有众多安全及网络基础设施方案供选择
- 强大的集中式管理
- 内置 IPSec 和 SSL VPN

## FORCEPOINT NGFW 规格

| 支持的平台 | |
|---|---|
| **硬件设备** | 有多种硬件设备方案，包括在分支机构和数据中心部署 |
| **软件设备** | 基于 X86 的系统 |
| **虚拟设备** | 支持 VMware ESX、Oracle VM 和 KVM |
| **支持的角色** | • 带 NGF 许可证：防火墙 / VPN（第 3 层）、IPS 模式（第 2 层）、第 2 层防火墙<br>• 带 FWL 许可证：防火墙 / VPN（第 3 层） |
| **虚拟情景（仅限 NGF 许可证）** | 进行虚拟化，以区分具有独立接口、地址、路由和策略的逻辑情景（防火墙、IPS 或第 2 层防火墙） |
| **防火墙 / VPN 功能角色** | |
| **常规** | 有状态和无状态数据包过滤，带有 TCP 代理协议代理程序的电路层防火墙 |
| **用户验证** | 内部用户数据库、LDAP、Microsoft Active Directory、RADIUS、TACACS+ |
| **高可用性** | • 主用-主用 / 主用-备用防火墙集群包含多达 16 个节点<br>• 有状态失效备援（包括 VPN 连接）<br>• 虚拟路由器冗余协议 (VRRP)<br>• 服务器负载均衡<br>• 链路聚合 (802.3ad)<br>• 链路故障检测 |
| **ISP 多归属** | 多链路：高可用性，多个 ISP（包括 VPN 连接）之间的负载均衡，多链路 VPN 链路聚合，基于 QoS 的链路选择 |
| **IP 地址分配** | • 防火墙集群：静态，IPv4、IPv6<br>• 防火墙单节点：静态（DHCP、PPoA、PPoE）IPv6（静态，SLAAC）<br>• 服务：适用于 IPv4 的 DHCP 服务器和 DHCP 中继 |
| **地址转换** | • IPv4、IPv6<br>• 静态 NAT、带端口地址转换 (PAT) 的源 NAT、带 PAT 的目标 NAT |
| **路由** | 静态 IPv4 和 IPv6 路由、基于策略的路由、静态组播路由 |
| **动态路由** | IGMP 代理、RIPv2、RIPng、OSPFv2、OSPFv3、BGP、PIM-SM |
| **IPv6** | 双栈 IPv4/IPv6、ICMPv6、DNSv6 |
| **SIP** | 允许 RTP 媒体流动态传输，NAT 遍历，深度检测，可与符合 RFC3261 标准的 SIP 设备互操作 |
| **CIS 重定向** | HTTP、FTP、SMTP 协议重定向到内容检测服务器 (CIS) |

## FORCEPOINT NGFW 规格（续）

| IPsec VPN | |
|---|---|
| **协议** | IKEv1、IKEv2 以及带 IPv4 和 IPv6 的 IPsec |
| **加密** | AES-128、AES-256、AES-GCM-128、AES-GCM-256、Blowfish、DES、3DES[1] |
| **消息摘要算法** | AES-XCBC-MAC、MD5、SHA-1、SHA-2-256、SHA-2-512 |
| **Diffie-Hellman** | DH 第 1、第 2 组、第 5 组、第 14 组、第 19 组、第 20 组、第 21 组 |
| **验证** | RSA、DSS、带 X.509 证书的 ECDSA 签名、预共享密钥、混合验证、扩展验证、EAP |
| **其他** | • IPCOMP deflate 压缩<br>• NAT-T<br>• 失效对等体检测<br>• MOBIKE |
| **站点到站点 VPN** | • 基于策略的 VPN、基于路由的 VPN（GRE、IP-IP、SIT）<br>• 中心辐射型拓扑、全网状拓扑、半网状拓扑<br>• 基于模糊逻辑的 Forcepoint Multi-Link 动态链路选择<br>• Forcepoint Multi-Link 模式：负载共享，主动 / 备用，链路聚合 |
| **移动 VPN** | • 适用于 Microsoft Windows 的 VPN 客户端<br>• 可从任何网关自动更新配置<br>• 多链路自动失效备援<br>• 客户端安全检查<br>• 安全域登录 |
| **SSL VPN**（仅限 NGF 许可证） | |
| **基于客户端的访问** | • 支持的平台：Android 4.0、Mac OS X 10.7 和 Windows Vista SP2（及更新版本） |
| **基于门户的访问** | • 使用浏览器通过 SSL VPN 门户访问 Outlook Web Access (OWA) 和内联网 |

## FORCEPOIT NGFW 规格（续）

| 检测 | |
|---|---|
| **防僵尸网络** | • 基于解密的检测<br>• 消息长度序列分析 |
| **动态情景检测** | 协议、应用、文件类型 |
| **高级防恶意软件** | 基于策略的文件过滤 |
| 沙盒 | 支持 McAfee Advanced Threat Defense |
| 文件信誉 | 来自 McAfee GTI 云服务的分类，或来自本地 McAfee Threat Information Exchange 的分类 |
| 防恶意软件引擎 | McAfee Anti-Malware Engine。扫描的协议：FTP、HTTP、HTTPS、POP3、IMAP、SMTP |
| **协议特定规范化 / 检测 / 流量处理[3]** | 以太网、H.323、GRE、IPv4、IPv6、ICMP、IP-in-IP、IPv6 封装、UDP、TCP、DNS、FTP、HTTP、HTTPS、IMAP、IMAPS、MGCP、Modbus/TCP、MSRPC、NetBios 数据报、OPC Classic、OPC UA、Oracle SQL Net、POP3、POP3S、RSH、RSTP、SIP、SMTP、SSH、SunRPC、NBT、SCCP、SMB、SMB2、SIP、TCP 代理、TFTP |
| **独立于协议的指纹识别** | 任何 TCP/UDP 协议 |
| **规避和异常检测** | • 多层流量规范化<br>• 基于漏洞的指纹<br>• 基于软件的完全可升级检测引擎<br>• 规避和异常记录 |
| **自定义指纹识别** | • 独立于协议的指纹匹配<br>• 基于正则表达式的指纹语言<br>• 自定义应用指纹识别 |
| **TLS 检测** | • HTTPS 客户端和服务器流式解密及检测<br>• TLS 证书有效性检查<br>• 基于证书域名的豁免清单 |
| **相关性** | 本地相关性、日志服务器相关性 |
| **DoS/DDoS 攻击防护** | • SYN/UDP 洪水攻击检测<br>• 并发连接限制，基于接口的日志压缩<br>• 防御慢速 HTTP 请求方法 |
| **侦察** | TCP/UDP/ICMP 扫描，隐形病毒检测，以及对 Ipv4 和 Ipv6 进行慢速扫描检测 |
| **拦截方法** | 直接拦截，重置连接，列入黑名单（本地黑名单和分布式黑名单），HTML 响应，HTTP 重定向 |
| **流量记录** | 自动流量记录 / 记录有关流量误用情况的摘要 |
| **更新** | • 通过 Forcepoint NGFW Security Management Center 自动进行动态更新<br>• 更新范围目前涵盖大约 4,700 个受保护的漏洞 |

## FORCEPOIT NGFW 规格（续）

| URL 过滤 | |
|---|---|
| **协议** | HTTP、HTTPS |
| **引擎** | 基于 Webroot 类别的 URL 过滤，黑名单 / 白名单 |
| **数据库** | • 超过 2.8 亿个顶级域和子页（数十亿个 URL）<br>• 支持超过 43 种语言和 82 个类别 |
| **安全搜索** | 通过强制使用谷歌、必应、雅虎、DuckDuckGo 网络搜索来实现安全搜索 |
| **管理和监控** | |
| **管理界面** | • 企业级集中管理、记录和报告系统。<br>• 详情请参阅 Forcepoint NGFW Security Management Center 产品资料。 |
| **SNMP 监控** | SNMPv1、SNMPv2c 和 SNMPv3 |
| **流量捕获** | 控制台 tcpdump，通过 SMC 远程捕获 |
| **高安全性管理通信** | 引擎管理通信采用 256 位安全强度 |
| **安全认证** | 通用标准 EAL4+、FIPS 140-2 加密证书、法国网络和信息安全局 (ANSSI) 提供的 CSPN 认证（一级安全认证 USGv6） |

[1] 支持的加密算法取决于使用的许可证。
[2] 仅限防火墙 / VPN 角色。
[3] 请参阅与防火墙许可证相关的限制。

**联系信息**
**www.forcepoint.com/contact**

**关于 FORCEPOINT**



[DATASHEET_FORCEPOINT_NGFW_SCH] 100033SCH.030117